

IN THE CLAIMS:

Claims 1, 2, and 33 are amended. No claims are cancelled or added. All pending claims and their present status are produced below.

1 1. (Currently amended) A method for providing a unique identification of monitored
2 network data instances flowing across various connections between networked
3 devices, the unique identification being derived from information contained entirely
4 within each instance of the network data, the method comprising:
5 using at least one monitoring device to monitor a network data instance flowing
6 across at least one data connection;
7 deriving from the data instance certain information which collectively provides a
8 unique identification of the network data instance;
9 assembling the derived information into an input string for a hash function; and
10 using the output string of the hash function as a signature which represents a unique
11 ~~identifer~~ identifier of the network data instance.

1 2. (Currently amended) The method according to Claim 1, wherein the deriving step
2 includes:
3 deriving from the data instance a source and destination address for the data;
4 deriving from the data instance a source and destination port associated with the
5 networked devices;
6 deriving from the data instance at least one sequence number associated with data
7 instance[;].

- 1 3. (Original) The method according to Claim 1, which further includes:
2 attaching the signature to at least one data report associated with the network data
3 instance; and
4 transmitting the data reports and signatures from each monitoring device to a central
5 collecting device.
- 1 4. (Original) The method according to Claim 3, wherein a timestamp is further
2 associated with each data report before it is transmitted to the central collector.
- 1 5. (Original) The method according to Claim 3, wherein the central collecting device
2 uses the signatures to eliminate duplicate data reports that might come in from
3 different monitoring devices positioned at different locations on the network.
- 1 6. (Original) The method according to Claim 1, wherein network data instances are data
2 packets as part of a TCP/IP (Transmission Control Protocol/Internet Protocol) client-
3 server network.
- 1 7. (Original) The method according to Claim 6, wherein the source and destination
2 addresses include a client IP address and a server IP address.
- 1 8. (Original) The method according to Claim 7, wherein the source and destination port
2 include a client port number and a server port number.
- 1 9. (Previously Presented) The method according to Claim 2, wherein the at least one
2 sequence number includes a client sequence number or a server sequence number.
- 1 10. (Original) The method according to Claim 9, wherein the at least one sequence
2 number includes both a client sequence number and a server sequence number.
- 1 11. (Original) The method according to Claim 2, wherein the input string information
2 does not include sequence numbers.

- 1 12. (Original) The method according to Claim 11, wherein the network data instances are
2 datagrams as part of a UDP/IP (User Datagram Protocol/Internet Protocol) network.
- 1 13. (Original) The method according to Claim 1, which further includes: truncating the
2 signature to include fewer bits than the hash function output string.
- 1 14. (Original) The method according to Claim 1, which further includes: adding flag bits
2 to the signature which indicate the type of application associated with the network
3 data instance.
- 1 15. (Original) The method according to Claim 3, wherein the monitor serves as a data
2 reduction device for data report and signature information being sent to the central
3 data collector.
- 1 16. (Original) The method according to Claim 1, wherein the monitoring device operates
2 to directly monitor the network data.
- 1 17. (Original) The method according to Claim 1, wherein the monitoring device operates
2 to indirectly monitor the network data.
- 1 18. (Original) An apparatus for providing a unique identification of monitored network
2 data instances flowing across various connections between networked devices, the
3 unique identification being derived from information contained entirely within each
4 instance of the network data, the apparatus comprising:
5 at least one monitoring device positioned to monitor a network data instance flowing
6 across at least one data connection;
7 a hash function device having an input string and an output string, the input string
8 assembled from certain information derived from the network data instance,

9 the information collectively providing a unique identification of the network
10 data instance;
11 wherein the output string is used as a signature which represents a unique identifier of
12 the network data instance.

1 19. (Original) The apparatus according to Claim 18, wherein information derived from
2 the network data instance includes at least:
3 a source and destination address derived from the network data instance;
4 a source and destination port associated with the networked devices; and
5 at least one sequence number associated with network data instance.

1 20. (Original) The apparatus according to Claim 18, which further includes:
2 at least one data report associated with the network data instance, the signature being
3 attached to the data report; and
4 a central collection device that receives transmitted data reports and signatures from
5 each monitoring device.

1 21. (Original) The apparatus according to Claim 20, wherein a timestamp is further
2 associated with each data report before it is transmitted to the central collector.

1 22. (Original) The apparatus according to Claim 20, wherein the central collecting
2 device uses the signatures to eliminate duplicate data reports that might come in from
3 different monitoring devices positioned at different locations on the network.

1 23. (Previously presented) The apparatus according to Claim 19, wherein network data
2 instances are data packets as part of a TCP/IP (Transmission Control
3 Protocol/Internet Protocol) client-server network.

- 1 24. (Original) The apparatus according to Claim 23, wherein the source and destination
2 addresses include a client IP address and a server IP address.
- 1 25. (Original) The apparatus according to Claim 24, wherein the source and destination
2 port include a client port number and a server port number.
- 1 26. (Original) The apparatus according to Claim 25, wherein the at least one sequence
2 number includes a client sequence number or a server sequence number.
- 1 27. (Original) The apparatus according to Claim 26, wherein the at least one sequence
2 number also includes both a client sequence number and a server sequence number.
- 1 28. (Original) The apparatus according to Claim 19, wherein the input string information
2 does not include sequence numbers.
- 1 29. (Original) The apparatus according to Claim 28, wherein the network data instances
2 are datagrams as part of a UDP/IP (User Datagram Protocol/Internet Protocol)
3 network.
- 1 30. (Original) The method according to Claim 18, wherein the signature is truncated to
2 include fewer bits than the hash function output string.
- 1 31. (Original) The method according to Claim 18, wherein flag bits are added to the
2 signature which indicate the type of application associated with the network data
3 instance.
- 1 32. (Original) The method according to Claim 20, wherein the monitor serves as a data
2 reduction device for data report and signature information being sent to the central
3 data collector.
- 1 33. (Currently amended) A method for providing a unique signature of monitored
2 network data packets flowing across various connections between networked devices,

3 the unique signature being derived from information contained entirely within each
4 instance of the network data packet, the method comprising:
5 using at least one monitoring device to monitor a network data packet flowing across
6 at least one data connection;
7 deriving from the data packet a source and destination address for the data;
8 deriving from the data packet a source and destination port associated with the
9 networked devices;
10 deriving from the data packet at least one sequence number associated with data
11 instance;
12 assembling the derived addresses, ports, and at least one sequence number
13 information into an input string for a hash function; and
14 using the output string of the hash function as the signature which represents a unique
15 ~~identifer~~ identifier of the network data packet[.];
16 attaching the signature to at least one data report associated with the network data
17 packet; and
18 transmitting the data reports and signatures from each monitoring device to a central
19 collecting device for analysis.